ELSEVIER

Discrete Mathematics 240 (2001) 161–173

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Factorizations of root-based polynomial compositions

Donald Mills *,[1]

U.S. Army Research Laboratory, Aberdeen Proving Ground, Aberdeen, MD 21005, USA

Received 10 May 1999; revised 18 May 2000; accepted 28 August 2000

Abstract

Let $\mathbb{F}_q$ denote the finite field of order $q = p^r$, p a prime and r a positive integer, and let $f(x)$ and $g(x)$ denote monic polynomials in $\mathbb{F}_q[x]$ of degrees m and n, respectively. Brawley and Carlitz (Discrete Math. 65 (1987) 115–139) introduce a general notion of root-based polynomial composition which they call the *composed product* and denote by $f \diamondsuit g$. They prove that $f \diamondsuit g$ is irreducible over $\mathbb{F}_q$ if and only if f and g are irreducible with $\gcd(m,n)=1$. In this paper, we extend Brawley and Carlitz's work by examining polynomials which are composed products of irreducibles of non-coprime degrees. We give an upper bound on the number of distinct factors of $f \diamondsuit g$, and we determine the possible degrees that the factors of $f \diamondsuit g$ can assume. We also determine when the bound on the number of factors of $f \diamondsuit g$ is met.

MSC: primary 12E10; secondary 11T06

Keywords: Finite fields; Polynomial composition; Polynomial factorization

1. Introduction

Let $\mathbb{F}_q$ denote the finite field of order $q = p^r$, p a prime and r a positive integer, and let $f(x)$ and $g(x)$ denote monic polynomials in $\mathbb{F}_q[x]$. The *composed sum* of f and g is the polynomial defined by

$$f * g = \prod_{\alpha} \prod_{\beta} (x - (\alpha + \beta)) \tag{1.1}$$

* Correspondence address: Mathematical Sciences Dept., USMA, West Point, NY 10996, USA. Tel.: +1-845-938-7830.

E-mail address: ad3943@usma.edu, ddmills@arl.army.mil (D. Mills).

[1] The author wrote this paper while he was a graduate student in the Department of Mathematical Sciences at Clemson University in Clemson, SC. He is now a Davies Fellow for the National Research Council, with joint appointments at the United States Military Academy and the U.S. Army Research Laboratory. He wishes to thank the NRC, and specifically ARL, for the use of their facilities during the time that this paper was revised.

0012-365X/01/$ - see front matter
PII: S0012-365X(00)00389-7

while the *composed multiplication* of f and g is the polynomial defined by

$$f \circ g = \prod_{\alpha} \prod_{\beta} (x - \alpha\beta). \tag{1.2}$$

In both cases, the product runs through all roots α of f and β of g, including multiplicities.

In [1] these compositions are generalized as follows. Let G be a nonempty subset of the algebraic closure Γ_q of $\mathbb{F}_q$ with the property that G is invariant under the Frobenius automorphism $\alpha \mapsto \sigma(\alpha) = \alpha^q$. Suppose there is defined on G a binary operation $\diamondsuit$ satisfying

$$\sigma(\alpha \diamondsuit \beta) = \sigma(\alpha) \diamondsuit \sigma(\beta) \tag{1.3}$$

for all $\alpha, \beta \in G$. Let $M_G[q,x]$ denote the set of monic polynomials whose coefficients are in $\mathbb{F}_q$ and whose roots lie in G. The *composed product* of f and g, denoted $f \diamondsuit g$, is the polynomial defined by

$$f \diamondsuit g = \prod_{\alpha} \prod_{\beta} (x - (\alpha \diamondsuit \beta)), \tag{1.4}$$

where the $\diamondsuit$-products are over all roots α of f and β of g. It is clear that

$$\deg f \diamondsuit g = (\deg f)(\deg g)$$

and it is also clear that when $G = \Gamma_q$ and $\diamondsuit$ is the usual addition (respectively, the usual multiplication) on Γ_q, then (1.4) becomes (1.1) (respectively (1.2)).

While the roots of f and g are in G and not necessarily in $\mathbb{F}_q$, it is easy to prove that (1.3) implies that the composed product (1.4) has its coefficients in $\mathbb{F}_q$ [1]. Further, under the additional assumption that G is a group under $\diamondsuit$, the composition (1.4) has the following property which allows for the construction of irreducibles in $\mathbb{F}_q[x]$ of large degree from irreducibles of smaller degrees.

Theorem 1.1 (Brawley and Carlitz [1]). *Let* $(G, \diamondsuit)$ *be a* σ*-invariant group satisfying* (1.3) *and let* f, g *be monic polynomials in* $M_G[q,x]$ *of degrees* m *and* n*, respectively. Then the composed product* $f \diamondsuit g \in M_G[q,x]$ *is irreducible if and only if* f *and* g *are irreducible and* $\gcd(m,n) = 1$.

The proof of Theorem 1.1 uses the following property among other things: If f and g factor over $\mathbb{F}_q$ as $f = f_1 f_2 \cdots f_s$ and $g = g_1 g_2 \cdots g_t$, then

$$\left(\prod_{i=1}^{s} f_i\right) \diamondsuit \left(\prod_{j=1}^{t} g_j\right) = \prod_{i=1}^{s} \prod_{j=1}^{t} (f_i \diamondsuit g_j). \tag{1.5}$$

We examine the factorization of $f \diamondsuit g$ when the degrees of the irreducibles f and g are not coprime. There is sufficient motivation to consider this problem, particularly for the case of composed multiplication, as this problem relates to finding the minimal polynomial of the product of linear recurring sequences. Lidl and Niederreiter

[5, pp. 433–435] show how to find a characteristic polynomial for the product of homogeneous linear recurring sequences. Specifically, they show that for any given pair of nonconstant polynomials $f(x), g(x) \in \mathbb{F}_q[x]$ and for any pair of linear recurring sequences $\{s_k\}$ and $\{t_k\}$ having characteristic polynomials $f(x)$ and $g(x)$, respectively, $f \circ g$ is a characteristic polynomial for the product sequence $\{s_k t_k\}$. Göttfert and Niederreiter [4] give results which produce a lower bound on the degree, or linear complexity, of the minimal polynomial of the product sequence. Göttfert and Niederreiter note that it is an important problem in the theory of stream ciphers to determine the linear complexity of sequences obtained by componentwise multiplication of other sequences, and also point out that it is a worthwhile goal to obtain a characteristic polynomial for the product sequence, as the degree of the characteristic polynomial provides an upper bound on the product sequence's linear complexity. This serves as ample motivation for their work, and also for the results given in this paper as well, particularly since the polynomials used to generate the composed multiplication here are irreducible polynomials and therefore 'nice' polynomials to work with. Determining an upper bound on the number of distinct factors of the composed multiplication of two irreducibles, producing conditions under which this bound is met, and ascertaining the possible degrees of the irreducible factors of the composed multiplication, then, are all worthwhile goals when placed in the context of determining the minimal polynomial of a product sequence for which the composed multiplication serves as a characteristic polynomial.

In Section 2, we give an upper bound on the number of distinct factors of $f \diamondsuit g$, and in Section 3, we determine the possible degrees that the factors of $f \diamondsuit g$ can assume. In Section 4, we give conditions under which the bound of Section 2 is met, and specialize to $f * g$ and $f \circ g$. In the sections to follow, $(G, \diamondsuit)$ denotes a σ-invariant abelian group satisfying (1.3), $f, g \in M_G[q,x]$ denote irreducibles of degrees m and n, respectively, and with roots α and β, respectively, $d = \gcd(m,n)$, and $h = \mathrm{lcm}(m,n)$. The restriction that G be an abelian group is done for convenience's sake, particularly since we are most interested in the case in which G is either an additive or multiplicative group, but it should be noted that neither Theorem 2.1 nor Theorem 3.1 require G to be abelian.

2. A bound on the number of factors of $f \diamondsuit g$

Another way to state the result of Theorem 1.1 is that if the degrees of the irreducibles $f, g \in M_G[q,x]$ are coprime, then the factorization of their composed product yields one irreducible factor of multiplicity one. Thus, the following generalization of Theorem 1.1.

Theorem 2.1. *The number of distinct irreducible factors of $f \diamondsuit g$ which lie in $M_G[q,x]$ is at most d, and the degree of each factor divides h.*

Proof. Let α represent a root of f and β a root of g, so that the mn roots of $f \diamondsuit g$ are given by $\{\alpha^{q^u} \diamondsuit \beta^{q^v}\}$, $0 \leqslant u \leqslant m-1$ and $0 \leqslant v \leqslant n-1$. Certainly, $f \diamondsuit g$ has the factorization

$$f \diamondsuit g = \prod_{i=0}^{d-1} f_i(x),$$

where

$$f_i(x) = \prod_{k=0}^{h-1} (x - (\alpha \diamondsuit \beta^{q^i})^{q^k})$$

for each i. Since $\deg(\alpha \diamondsuit \beta^{q^i})$ divides h for all i, it is clear that $f_i(x) \in M_G[q,x]$ for each i. If $\deg(\alpha \diamondsuit \beta^{q^i}) = h/r$ for some integer $r > 1$, then $f_i(x)$ factors as $p_i^r(x)$ where $p_i(x) \in M_G[q,x]$ is irreducible of degree h/r. Standard number-theoretic arguments can be used now to show that, given a pair $(u,v) \in \mathbb{Z} \times \mathbb{Z}$ where $0 \leqslant u \leqslant m-1$ and $0 \leqslant v \leqslant n-1$, there exists a unique pair $(i,k) \in \mathbb{Z} \times \mathbb{Z}$, $0 \leqslant i \leqslant d-1$ and $0 \leqslant k \leqslant h-1$, such that $\alpha^{q^u} \diamondsuit \beta^{q^v} = (\alpha \diamondsuit \beta^{q^i})^{q^k}$. □

3. The degrees of the factors of $f \diamondsuit g$

We ask the following: What are the possible degrees of the irreducible factors of $f \diamondsuit g$? To answer this question, set $\bar{m} = m/d$ and $\bar{n} = n/d$, let $\bar{d}$ represent the largest factor of d such that $\gcd(\bar{d}, \bar{m}) = \gcd(\bar{d}, \bar{n}) = 1$, and use the number $\bar{d}$ to define the set $\bar{D} = \{h/l : l \in \mathbb{Z}^+, l | \bar{d}\}$. Further, let $\mathscr{M}$ and $\mathscr{N}$ represent the sets of all irreducibles of degrees m and n in $M_G[q,x]$, respectively, and put $\mathscr{M} \diamondsuit \mathscr{N} = \{f \diamondsuit g : f \in \mathscr{M},\ g \in \mathscr{N}\}$. Finally, let $H_{m,n}$ represent the set of the degrees of the irreducible factors of each of the compositions in $\mathscr{M} \diamondsuit \mathscr{N}$.

Theorem 3.1. *Suppose $\bar{m}, \bar{n}, \bar{d}, \bar{D}, \mathscr{M}, \mathscr{N}$, and $H_{m,n}$ are defined as above. Then $H_{m,n} \subseteq \bar{D}$.*

Proof. Assume without loss of generality (hereafter WLOG) that $m \neq n$, for otherwise $h = m = n = \bar{d} = d$, and hence $H_{m,n} \subseteq \bar{D}$.

Suppose to the contrary that $H_{m,n}$ is not contained in $\bar{D}$. Then there exists α, $\beta \in G$ of degrees m and n, respectively, and an integer $t \in H_{m,n} \backslash \bar{D}$ such that $(\alpha \diamondsuit \beta)^{q^t} = \alpha \diamondsuit \beta$. Writing t as $t = h/w$ where $w \in \mathbb{Z}^+$, we see that since h/w is not in $\bar{D}$, either $\gcd(w, \bar{m}) > 1$ or $\gcd(w, \bar{n}) > 1$. Suppose WLOG that $\gcd(w, \bar{m}) > 1$, and let w_1 represent the gcd of w and $\bar{m}$. Factoring $\bar{m}$ and w as $\bar{m} = m_1 w_1$ and $w = w_1 w_2$, we have

$$(\alpha \diamondsuit \beta)^{q^{m_1 n / w_2}} = \alpha \diamondsuit \beta. \tag{3.1}$$

Raising both sides of (3.1) to the $q^{m_1 n / w_2}$ power w_2 times, we obtain $(\alpha \diamondsuit \beta)^{q^{m_1 n}} = \alpha \diamondsuit \beta$. Since $m_1 < \bar{m}$, we have $m_1 n < h$, and since $(G, \diamondsuit)$ is a group, cancellation gives $\alpha^{q^{m_1 n}} = \alpha$. But this is a contradiction since the smallest integer v such that $\alpha^{q^{vn}} = \alpha$ is $v = \bar{m}$. □

We ask under what conditions $H_{m,n}=\bar{D}$. In order to answer this question, we assume the following:

(1) G contains elements of all prime power degrees corresponding to the prime powers contained in the factorizations of m and n.
(2) For each prime p and positive integer w, $|G_{p^w}| > 2|G_{p^{w-1}}|$ where $G_r = G \cap \mathbb{F}_{q^r}$ for $r \in \mathbb{Z}^+$. Note that G_r is a subgroup of G [3]. Note as well that, since r is a power of a prime here, the requirement that $|G_{p^w}| > 2|G_{p^{w-1}}|$ is by no means an unduly restrictive one.

Denote these properties by $P1$ and $P2$, respectively. We also require Lemma 3.2, which is given below. Before we state and prove the lemma, we write the prime factorizations of m and n as

$$m = (p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s})(q_1^{u_1} q_2^{u_2} \cdots q_t^{u_t}) \tag{3.2}$$

and

$$n = (p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s})(r_1^{v_1} r_2^{v_2} \cdots r_w^{v_w}) \tag{3.3}$$

with $p_i \neq p_j$ for all $i \neq j$, $q_k \neq r_l$ for all choices of k and l, and with $d = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$, so that $\bar{d} = p_1^{\bar{e}_1} p_2^{\bar{e}_2} \cdots p_s^{\bar{e}_s}$, $\bar{e}_i \leqslant e_i$ for all i. Further, we write the number l found in the definition of $\bar{D}$ as $l = \prod_{i=1}^{s} p_i^{b_i}$, $0 \leqslant b_i \leqslant \bar{e}_i$ for each i.

Lemma 3.2. *Let $(G, \diamondsuit)$ be a σ-invariant group satisfying* (1.3) *and properties $P1$ and $P2$, and suppose the factorizations of m and n are given by* (3.2) *and* (3.3), *respectively. Let $\bar{d}$ and l be defined as in Theorem* 3.1, *and suppose that the factorizations of d, $\bar{d}$, and l are given as above. For i from* 1 *to s, select an element $\alpha_i \in G$ of degree $p_i^{e_i}$. If $b_i > 0$, then there exists an element $\delta_i \in G$ of degree $p_i^{e_i - b_i}$ such that $\beta = \bar{\alpha}_i \diamondsuit \delta_i$ has degree $p_i^{e_i}$, where $\bar{\alpha}_i$ is the group inverse of α_i under $\diamondsuit$. If $b_i = 0$ and $|G_{p_i^{e_i}}| > 2|G_{p_i^{e_i-1}}|$, then there exists an element $\delta_i \in G$ of degree $p_i^{e_i}$ such that $\beta_i = \bar{\alpha}_i \diamondsuit \delta_i$ has degree $p_i^{e_i}$.*

Proof. The case $e_i = 0$ is trivial, so we assume $e_i \geqslant 1$. As indicated in the statement of the lemma, there are two cases.

(1) $b_i > 0$. Since b_i is positive, $G_{p_i^{e_i - b_i}}$ is a proper subgroup of $G_{p_i^{e_i}}$. Select α_i, δ_i in $G_{p_i^{e_i}}$, where $\deg(\alpha_i) = p_i^{e_i}$ and $\deg(\delta_i) = p_i^{e_i - b_i}$. Since we know that $\deg(\alpha_i) = \deg(\bar{\alpha}_i)$, and since the degrees of $\bar{\alpha}_i$ and δ_i are prime powers, it follows that $\deg(\bar{\alpha}_i \diamondsuit \delta_i) = p_i^{e_i}$.
(2) $b_i = 0$. In this case, we seek elements δ_i, $\alpha_i \in G$ such that $\deg(\delta_i) = \deg(\bar{\alpha}_i)$ with $\deg(\beta_i) = p_i^{e_i}$, where $\beta_i = \bar{\alpha}_i \diamondsuit \delta_i$. To show that we can find such elements in G, consider the subgroups $\Phi = G_{p_i^{e_i}}$ and $\Lambda = G_{p_i^{e_i-1}}$, and put $A = |\Phi|$ and $B = |\Lambda|$. By hypothesis, $A > 2B$, so there exist elements ρ_1, $\rho_2 \in \Phi \backslash \Lambda$ such that the cosets $\rho_1 \Lambda$ and $\rho_2 \Lambda$ are disjoint, and it follows that $\rho_3 = \rho_1 \diamondsuit \bar{\rho}_2 \in \Phi \backslash \Lambda$. Finally, we set $\rho_1 = \delta_i$, $\rho_2 = \alpha_i$, and $\rho_3 = \beta_i$. □

Theorem 3.3. *Let* $(G, \diamondsuit)$ *be a* σ*-invariant group satisfying* (1.3) *and properties* $P1$ *and* $P2$*, and suppose that the factorizations of* m *and* n *are given by* (3.2) *and* (3.3)*, respectively. Further, let* $\mathscr{M}, \mathscr{N}, \mathscr{M} \diamondsuit \mathscr{N}, H_{m,n}$ *and* $\bar{D}$ *be defined as in Theorem* 3.1. *Then* $\bar{D} \subseteq H_{m,n}$.

Proof. Select an arbitrary element h/l from $\bar{D}$, and refer to (3.2) and (3.3). By Lemma 3.2, for each prime power of m, we can select an element $\alpha_i \in G$ of degree equal to that prime power, and likewise for each prime power of n we can select an element $\beta_i \in G$ of degree equal to that prime power. The stipulation we place on the elements α_i and β_i, $1 \leqslant i \leqslant s$ is that for each i, $\beta_i = \bar{\alpha}_i \diamondsuit \delta_i$ where $\deg(\delta_i) = p_i^{e_i - b_i}$. Referring to (3.2) and (3.3), let us suppose WLOG that $t \leqslant w$, with $q_{t+1} = \cdots = q_w = 1$. Setting $\alpha = \alpha_1 \diamondsuit \alpha_2 \diamondsuit \cdots \diamondsuit \alpha_{s+w}$ and $\beta = \beta_1 \diamondsuit \beta_2 \diamondsuit \cdots \diamondsuit \beta_{s+w}$, we have $\alpha \diamondsuit \beta = (\alpha_1 \diamondsuit \beta_1) \diamondsuit (\alpha_2 \diamondsuit \beta_2) \diamondsuit \cdots \diamondsuit (\alpha_{s+w} \diamondsuit \beta_{s+w})$. We note the following.

1. For i from 1 to s, $\deg(\alpha_i \diamondsuit \beta_i) = p_i^{e_i - b_i}$.
2. For j from 1 to w, $\deg(\alpha_j \diamondsuit \beta_j) = q_j^{u_j} r_j^{v_j}$.

By the definition of l, then, we have $\deg(\alpha \diamondsuit \beta) = h/l$. □

The stipulation given in Lemma 3.2 regarding the relative size of $G_{p_i^{e_i}}$ to $G_{p_i^{e_i - 1}}$ is necessary, for it could happen that $\alpha \diamondsuit \beta \in \Lambda$ for all choices α, $\beta \in \Phi \backslash \Lambda$. An example of this is the case where $q = p_i = 2$, $e_i = 1$, and $G_1 = \mathbb{F}_2$ is a subgroup of the additive group $(G_2, +) = (\mathbb{F}_4, +)$. In this case, $\Phi \backslash \Lambda$ consists of the elements α and its conjugate $\alpha^2 = \alpha + 1$, and we have $\alpha + \alpha = (\alpha + 1) + (\alpha + 1) = 0$ while $\alpha + \alpha + 1 = 1$.

Example 3.4. Let $m = 588 = 2^2 \cdot 3 \cdot 7^2$ and $n = 420 = 2^2 \cdot 3 \cdot 5 \cdot 7$, so that $d = 2^2 \cdot 3 \cdot 7 = 84$, $h = 2^2 \cdot 3 \cdot 5 \cdot 7^2 = 2940$, $\bar{m} = 7$, $\bar{n} = 5$ and $\bar{d} = 12$. Choosing $l = 6$, so that $(h/l) = 490$, we find elements α and β whose composed product is of degree 490. To do this, we select elements $\alpha_1, \alpha_2, \alpha_3$, and α_4 of degrees 4, 3, 1 and 49, respectively, for m, and then we select elements β_1, β_2, β_3, and β_4 of degrees 4, 3, 5 and 7, respectively, for n, with the stipulation that $\deg(\alpha_1 \diamondsuit \beta_1) = 2$ while $\deg(\alpha_2 \diamondsuit \beta_2) = 1$. Setting $\alpha = \alpha_1 \diamondsuit \alpha_2 \diamondsuit \alpha_3 \diamondsuit \alpha_4$ and $\beta = \beta_1 \diamondsuit \beta_2 \diamondsuit \beta_3 \diamondsuit \beta_4$, we see that $\deg(\alpha \diamondsuit \beta) = 490$.

We now determine when $f \diamondsuit g$ has an irreducible factor of degree strictly dividing the least common multiple of the degrees of f and g. To do this, we define a polynomial whose roots are group inverses of the roots of a given irreducible. Specifically, if f factors as $f(x) = \prod_\alpha (x - \alpha)$, we set $\bar{f} = \prod_\alpha (x - \bar{\alpha})$, where $\bar{\alpha}$ represents the inverse of α under $\diamondsuit$. We write g and $\bar{g}$ similarly, letting β represent a root of g.

Theorem 3.5. *Let* $\bar{f}$ *and* $\bar{g}$ *be defined as above, let* F *represent the set of distinct nonidentity roots of* $f \diamondsuit \bar{f}$*, let* U *represent the set of distinct nonidentity roots of* $g \diamondsuit \bar{g}$*, and let* H *represent the set of distinct roots of* $f \diamondsuit g$ *which have degree strictly dividing* h*. Then* $F \cap U \neq \emptyset$ *if and only if* $H \neq \emptyset$.

Proof. ($\Rightarrow$) The proof uses the usual correspondence arguments. First suppose that $F \cap U \neq \emptyset$, that is $f \diamondsuit \bar{f}$ and $g \diamondsuit \bar{g}$ have a nontrivial irreducible factor in common. By nontrivial we mean that the factor in question is something other than $x - e$, where e represents the identity element of G. Hence, there exist $r, s \in \mathbb{Z}^+$, $1 \leqslant r \leqslant n-1$ and $1 \leqslant s \leqslant m-1$ such that $\alpha^{q^s} \diamondsuit \bar{\alpha} = \beta \diamondsuit \bar{\beta}^{q^r}$ or

$$\alpha^{q^s} \diamondsuit \beta^{q^r} = (\alpha \diamondsuit \beta^{q^{r-s}})^{q^s} = \alpha \diamondsuit \beta. \tag{3.4}$$

From Theorem 2.1 we have $r \equiv s \bmod d$, so that $dw = r - s$ for some $w < \bar{n}$. From Theorem 2.1 and (3.4), it follows that there exists a $T < \deg(\alpha \diamondsuit \beta)$ such that $T \equiv 0 \bmod m$, $T \equiv r - s \bmod n$, and

$$(\alpha \diamondsuit \beta)^{q^T} = \alpha \diamondsuit \beta^{q^{r-s}}, \tag{3.5}$$

and hence

$$(\alpha \diamondsuit \beta)^{q^{T+s}} = \alpha \diamondsuit \beta. \tag{3.6}$$

Since $(\alpha \diamondsuit \beta)^{q^h} = \alpha \diamondsuit \beta$, we have $(T+s) | h$ or $h | (T+s)$. If $h | (T+s)$, then $h > T \geqslant h - s > h - m$, but if $h - m < T < h$ then $m \nmid T$, a contradiction. Hence $(T+s) \mid h$. Since $T < h$ and $s < m$, $(T+s) \mid h$ strictly, and hence $\alpha \diamondsuit \beta \in H$.

($\Leftarrow$) Suppose $H \neq \emptyset$, so that $\deg(\alpha \diamondsuit \beta) = r$ where $r \mid h$ strictly. Note that $m \nmid r$ and $n \nmid r$, for if $m \mid r$, say $mt = r$ for $t \in \mathbb{Z}^+$, then cancellation gives $\beta^{q^{mt}} = \beta$, which is impossible since $mt < h$. We have $(\alpha \diamondsuit \beta)^{q^r} = \alpha^{q^r} \diamondsuit \beta^{q^r} = \alpha \diamondsuit \beta$, so that $\alpha^{q^r} \diamondsuit \bar{\alpha} = \beta \diamondsuit \bar{\beta}^{q^r}$, and hence $F \cap U \neq \emptyset$. $\square$

One question to ask is whether $\bar{f}$ and $\bar{g}$ can be determined easily. If $(G, \diamondsuit)$ is a subgroup of either the additive group $(\Gamma_q, +)$ or the multiplicative group $(\Gamma_q^*, \cdot)$, the answer is yes. In particular, let $(G, \diamondsuit)$ be a subgroup of $(\Gamma_q, +)$ and set $f(x) = \sum_{i=0}^{n} c_i x^i \in M_G[q, x]$ with $c_n = 1$. Then it is not difficult to see that $\bar{f}(x) = \sum_{i=0}^{n} d_i x^i$ where if n is odd we have $d_i = -c_i$ for i from $n-1$ by 2 down to 0, and $d_i = c_i$ otherwise. A similar argument prevails when n is even; thus,

$$\bar{f}(x) = (-1)^n f(-x).$$

For the case in which $(G, \diamondsuit)$ is a subgroup of $(\Gamma_q^*, \cdot)$, it is a straightforward exercise to show that

$$\bar{f}(x) = c_0^{-1} x^n f(1/x).$$

Example 3.6. Let $(G, \diamondsuit)$ be a subgroup of $(\Gamma_3, +)$, and consider the irreducibles $f, g \in M_G[3, x]$ given by $f(x) = x^{15} + x^{13} + x^{12} + x^{11} + 2x^{10} + 2x^7 + x^6 + 2x^5 + 2x^2 + 2x + 1$ and $g(x) = x^{10} + 2x^9 + x^8 + x^7 + 2x^5 + x^4 + 2x^3 + x^2 + x + 2$. When we compute $f * \bar{f}$ and $g * \bar{g}$ (see [2] for efficient methods of computing composed products), we find that these composed sums share the irreducible factors $x^5 + 2x + 2$, $x^5 + 2x^3 + 2x^2 + x + 1$, $x^5 + 2x^3 + x^2 + x + 2$, and $x^5 + 2x + 1$. So by Theorem 3.5, $f * g$ has at least one irreducible factor of degree strictly dividing $\operatorname{lcm}(10, 15) = 30$. We compute $f * g$ with the result being a composed sum of degree 150 which has 5 distinct irreducible factors, 4 of degree 30 and one of degree 6.

4. Determining when the bound of Theorem 2.1 is tight

A natural question to ask is whether it is possible for a given composed product's factorization to have fewer than the maximum possible number of distinct factors. In terms of the factorization given in the proof of Theorem 2.1, we give an equivalent form of this question: Is it possible for $(\alpha \diamondsuit \beta)^{q^k}$ to equal $\alpha \diamondsuit \beta^{q^i}$ for some $k \in \{1,2,\ldots,h-1\}$ and $i \in \{1,2,\ldots,d-1\}$? In what follows, we assume that k and i are chosen to be minimal.

4.1. The general case

Suppose that for some $k \in \{1,2,\ldots,h-1\}$ and $i \in \{1,2,\ldots,d-1\}$ we have

$$(\alpha \diamondsuit \beta)^{q^k} = \alpha \diamondsuit \beta^{q^i}. \tag{4.1}$$

Note that $m \nmid k$, for otherwise $\beta^{q^{sm}} = \beta^{q^i}$ for some positive integer s, and hence $n \mid (sm-i)$. But then $d \mid i$, a contradiction. Note also that (4.1) implies

$$\alpha^{q^k} \diamondsuit \bar{\alpha} = \beta^{q^i} \diamondsuit \bar{\beta}^{q^k} = \gamma, \tag{4.2}$$

where $\bar{\alpha}$ and $\bar{\beta}$ are the group inverses of α and β, respectively, and $\gamma \in G_d$, with G_d defined as in Lemma 3.2.

Assuming (4.1) holds, we find a necessary condition on the values of k and i. As a partial converse, we select k, i, d and γ and then determine the degrees of α and β over $\mathbb{F}_q$ which allow (4.1) to hold. We state the necessary condition first.

Theorem 4.1. *Let* $s = \deg(\alpha^{q^d} \diamondsuit \bar{\alpha})$ *and* $r = \deg(\beta^{q^d} \diamondsuit \bar{\beta})$, *and suppose that* (4.1) *holds for some* k, i *and* γ *as described above. Then*

(1) $k \equiv 0 \bmod s$ *and* $k \equiv i \bmod r$.
(2) *At least one of* s *and* r *is not a multiple of* d

Proof. (1) From (4.2) we have $(\alpha^{q^k} \diamondsuit \bar{\alpha})^{q^d} = \alpha^{q^k} \diamondsuit \bar{\alpha}$ or $(\alpha^{q^d} \diamondsuit \bar{\alpha})^{q^k} = \alpha^{q^d} \diamondsuit \bar{\alpha}$, and since $s = \deg(\alpha^{q^d} \diamondsuit \bar{\alpha})$ it follows that $s|k$. It is similarly shown that $k \equiv i \bmod r$.

(2) From the proof of the first statement we have $st = k$ for some $t \in \mathbb{Z}^+$, and further that $r \mid (st - i)$ or $st - rw = i$ for some $w \in \mathbb{Z}^+$. If s and r are both divisible by d then $d \mid i$, a contradiction. Hence $s < m$ or $r < n$, or both. □

For the partial converse, suppose that for some $\alpha \in G$ we have $\alpha^{q^k} = \alpha \diamondsuit \gamma$. Then $\alpha^{q^{2k}} = \alpha^{q^k} \diamondsuit \gamma^{q^k} = \alpha \diamondsuit (\gamma \diamondsuit \gamma^{q^k})$, and in general we have $\alpha^{q^{vk}} = \alpha \diamondsuit (\gamma \diamondsuit \gamma^{q^k} \diamondsuit \cdots \diamondsuit \gamma^{q^{(v-1)k}})$ for all positive integers v. Put $\varepsilon = \gcd(k,d)$, so that $k = \varepsilon k_1$ and $d = \varepsilon d_1$. Note that $dk_1 = kd_1$. When $v = d_1$ we have

$$\alpha^{q^{kd_1}} = \alpha \diamondsuit \gamma_1,$$

where $\gamma_1 = \gamma \diamondsuit \gamma^{q^k} \diamondsuit \cdots \diamondsuit \gamma^{q^{(d_1-1)k}}$ is the $\diamondsuit$-norm of γ over $\mathbb{F}_{q^k}$ (see [3] for details on the $\diamondsuit$-norm; it is sufficient to think of the $\diamondsuit$-norm as simply a generalization of the usual trace and norm operations). If γ_1 is the identity of G then clearly $\deg(\alpha) \mid kd_1$.

Set $\kappa = |G_k|$, and note that for all $j \in \mathbb{Z}^+$ we have $\alpha^{q^{jkd_1}} = \alpha \diamondsuit [j](\gamma_1)$ where $[j](\gamma_1)$ represents γ_1 'diamonded' with itself j times. If $j = \kappa$, we have $\alpha^{q^{kd_1\kappa}} = \alpha$, and it follows that $\deg(\alpha) \mid kd_1\kappa$. To form a similar argument for β, suppose WLOG that $k > i$, set $\delta = \beta^{q^{k-i}} \diamondsuit \bar{\beta}$, and put $\rho = |G_{k-i}|$, with δ playing the role of γ now. Then $\deg(\beta) \mid d(k-i)_1\rho$ where $(k-i)_1$ plays the role of k_1. We state the result formally below.

Theorem 4.2. *Let $(G, \diamondsuit)$ be a σ-invariant group satisfying (1.3), let $d \in \mathbb{Z}^+$ and $\gamma \in \mathbb{F}_{q^d}$ be given, and select positive integers k and i where $i < d$ and WLOG $i < k$. Suppose that there are elements $\alpha, \beta \in G$ such that $\alpha^{q^k} = \alpha \diamondsuit \gamma$ and $\beta^{q^i} = \beta^{q^k} \diamondsuit \gamma$. Then $\deg(\alpha) \mid dk_1\kappa$ and $\deg(\beta) \mid d(k-i)_1\rho$ where κ, ρ, k_1 and $(k-i)_1$ are defined as above.*

In what follows, we specialize to the case in which $(G, \diamondsuit)$ is either a subgroup of $(\Gamma_q, +)$ or $(\Gamma_q^*, \cdot)$.

4.2. Composed multiplication

Let $(G, \diamondsuit)$ be a subgroup of $(\Gamma_q^*, \cdot)$, and suppose that for some $k \in \{1, 2, \ldots, h-1\}$ and $i \in \{1, 2, \ldots, d-1\}$ we have

$$(\alpha\beta)^{q^k} = \alpha\beta^{q^i}. \tag{4.3}$$

As with the general case, it is easy to show that m does not divide k. The necessary condition given in Theorem 4.1 can be stated here in terms of the orders of α and β. Specifically, put $A = \mathrm{ord}(\alpha)$ and $B = \mathrm{ord}(\beta)$, so that the order of q modulo A is m while the order of q modulo B is n, and further set $D = \gcd(A, B)$. Note that $D|(q^d - 1)$. Writing A and B as $A = D\bar{A}$ and $B = D\bar{B}$ with $\gcd(\bar{A}, \bar{B}) = 1$, the multiplicative analogue to Theorem 4.1 can be given as follows.

Theorem 4.3. *Let G be a subgroup of $(\Gamma_q^*, \cdot)$, and let $\alpha, \beta \in G$ be given. Set $A = \mathrm{ord}(\alpha)$ and $B = \mathrm{ord}(\beta)$ with $D = \gcd(A, B)$, $B = D\bar{B}$, and $A = D\bar{A}$. If (4.3) holds for some i and k as described above, then $\bar{B}|(q^i - q^k)$ and $\bar{A}|(q^k - 1)$ with $\mathrm{ord}(\alpha^{q^k-1}) = \mathrm{ord}(\beta^{q^i-q^k})$, that is*

$$\frac{A}{\gcd(A, q^k - 1)} = \frac{B}{\gcd(B, q^i - q^k)}.$$

Proof. If (4.3) holds, then $\alpha^{q^k-1} = \beta^{q^i-q^k}$ and hence $\beta^{A(q^i-q^k)} = \alpha^{B(q^k-1)} = 1$. It follows that $B|A(q^i - q^k)$ and $A|B(q^k - 1)$. Hence $\bar{B}|\bar{A}(q^i - q^k)$ and $\bar{A}|\bar{B}(q^k - 1)$, and since $\gcd(\bar{A}, \bar{B}) = \gcd(\bar{B}, q^i) = 1$, it follows that $\bar{B}|(q^i - q^k)$ and $\bar{A}|(q^k - 1)$. Also, $\mathrm{ord}(\alpha^{q^k-1}) = \mathrm{ord}(\beta^{q^i-q^k})$ clearly. □

A partial converse to Theorem 4.3 follows.

Theorem 4.4. *Let G be a subgroup of $(\Gamma_q^*,\cdot)$, let $m,n\in\mathbb{Z}^+$ be given, and put $d=\gcd(m,n)$. Select $\alpha,\beta\in G$ of degrees m and n, respectively, and with orders A and B, respectively. Set $D=\gcd(A,B)$, so that $A=D\bar{A}$ and $B=D\bar{B}$ with $\gcd(\bar{A},\bar{B})=1$. Suppose that for some $k\in\{1,2,\ldots,h-1\}$ and $i\in\{1,2,\ldots,d-1\}$ we have $\bar{B}|(q^i-q^k)$, $\bar{A}|(q^k-1)$, and $\operatorname{ord}(\alpha^{q^k-1})=\operatorname{ord}(\beta^{q^i-q^k})$. Then for some $w\in\mathbb{Z}^+$, $w<\operatorname{ord}(\alpha^{q^k}-1)$, we have $(\alpha^w\beta)^{q^k}=\alpha^w\beta^{q^i}$.*

Proof. Since $\bar{B}|(q^i-q^k)$ and $\bar{A}|(q^k-1)$, it follows that α^{q^k-1}, $\beta^{q^i-q^k}\in\mathbb{F}_{q^d}^*$. Since $\operatorname{ord}(\alpha^{q^k-1})=\operatorname{ord}(\beta^{q^i-q^k})$, it follows that α^{q^k-1} and $\beta^{q^i-q^k}$ are in the same subgroup of the multiplicative group $(\mathbb{F}_{q^d}^*,\cdot)$. Since this group is cyclic, there exists a positive integer $w<\operatorname{ord}(\alpha^{q^k-1})$ such that $(\alpha^{q^k-1})^w=\beta^{q^i-q^k}$. □

Theorem 4.3 gives us a necessary condition which suitably restricts k and i; we prove below that there is an alternate means of restricting the values of k and i. Assume (4.3) holds, so that $(\alpha^{q^k}/\alpha)=(\beta^{q^i}/\beta^{q^k})=\delta\in\mathbb{F}_{q^d}$. The first quotient $(\alpha^{q^k}/\alpha)=(\alpha^{q^{k+d}}/\alpha^{q^d})$, so that $\alpha^{1+q^{k+d}}=\alpha^{q^k+q^d}$ and hence $1+q^{k+d}\equiv q^k+q^d \bmod A$ where A represents the order of α. Rewrite this congruence as

$$(q^d-1)(q^k-1)\equiv 0 \bmod A. \tag{4.4}$$

We would like to determine which k satisfy this congruence. Write A as $A=A_1A_2$ where $A_1=\gcd(A,q^d-1)$, so that $((q^d-1)/A_1)(q^k-1)\equiv 0 \bmod A_2$. By definition of A_1 we have $\gcd(A_2,((q^d-1)/A_1))=1$, and hence $A_2|(q^k-1)$. Since $A_2|(q^m-1)$ as well, we have $A_2|(q^C-1)$ where $C=\gcd(k,m)$.

Set $A_0=\gcd(A_1,A_2)$, and write A_2 as $A_2=A_{21}A_{22}$ where every prime factor of A_{21} divides A_0, and $\gcd(A_0,A_{22})=1$. Hence A_{22} is the largest factor of A_2 such that $\gcd(A_1,A_{22})=1$. With these restrictions, A_{21} and A_{22} are uniquely chosen.

Lemma 4.5. *Under the conditions given above, $q^{\operatorname{lcm}(A_{21}d,C)}\equiv 1 \bmod A$, so long as A_0 is either odd or a multiple of 4.*

To prove Lemma 4.5, we require the following standard number-theoretic result. The proof of Lemma 4.6, which we will not give, is accomplished by induction on the value of ε.

Lemma 4.6. *Let p be a prime and q a prime power, with the restriction that $p=2$ and $q\equiv 3 \bmod 4$ do not simultaneously hold. Suppose that $p^e\,||\,(q^s-1)$ and $p^\varepsilon\,||\,r$, where by $p^z\,||\,r$ we mean that $p^z\,|\,r$ but $p^{z+1}\nmid r$. Then $p^{e+\varepsilon}||(q^{sr}-1)$.*

Proof. We prove Lemma 4.5 on the basis of A_0's value.

1. $A_0 = 1$. Hence $A_{21} = 1$, and since $q^d \equiv 1 \bmod A_1$ while $q^C \equiv 1 \bmod A_2$, it follows easily that $q^{\mathrm{lcm}(d,C)} \equiv 1 \bmod A$.
2. $A_0 > 1$. By Lemma 4.6, we have $q^{A_{21}d} \equiv 1 \bmod A_1A_{21}$. Further, $q^C \equiv 1 \bmod A_{22}$ as $q^C \equiv 1 \bmod A_2$. Since $\gcd(A_1A_{21}, A_{22}) = 1$, it follows that $q^{\mathrm{lcm}(A_{21}d,C)} \equiv 1 \bmod A$. □

Since m is the order of q modulo A, we have $m|\mathrm{lcm}(A_{21}d, C)$ and the condition on the value of k follows.

Theorem 4.7. *Suppose that for some $k \in \{1, 2, \ldots, h-1\}$ and $i \in \{1, 2, \ldots, d-1\}$ we have*

$$(\alpha\beta)^{q^k} = \alpha\beta^{q^i},$$

where k and i are chosen to be minimal. Then there exists a positive integer y such that $my = \mathrm{lcm}(A_{21}d, \gcd(k, m))$.

Theorem 4.7 assures us that the value of k is dependent upon the order of α in $\mathbb{F}^*_{q^m}$. We have an entirely similar condition for i provided that we modify (4.3) to read $(\alpha\beta)^{q^k} = \alpha\beta^{q^{i+k}}$ where i is now an unrestricted integer. We leave the details to the reader.

Example 4.8. We take our example from $\mathbb{F}_3$, with $m = 16$ and $n = 12$ so that $d = 4$. We use the irreducibles $f(x) = x^{16} + 2x^{12} + x^8 + x^4 + 2$ and $g(x) = x^{12} + x^{10} + x^2 + 2$ in this example; note that $\mathrm{ord}(f) = 320 = A$ and $\mathrm{ord}(g) = 112$, as can be verified using standard techniques.

Since $A = 320$, we have $A_1 = \gcd(320, 3^4 - 1) = 80$, and hence $A_2 = 4$. Thus $A_0 = 4$ as well, and hence $A_{21} = 4$, so that $A_{21}d = m$. Thus any value of k will cause $\mathrm{lcm}(A_{21}d, \gcd(k, m))$ to be a multiple of m. We have

$$\begin{aligned} f \circ g = {} & x^{192} + x^{188} + x^{180} + x^{168} + x^{164} + x^{160} + 2x^{156} + 2x^{152} + x^{148} + x^{144} \\ & + 2x^{136} + x^{132} + x^{128} + x^{124} + x^{120} + x^{116} + 2x^{112} + x^{100} + 2x^{96} + 2x^{92} \\ & + 2x^{88} + x^{84} + 2x^{80} + 2x^{76} + x^{68} + 2x^{44} + 2x^{40} + x^{36} + x^{32} + 2x^{28} \\ & + 2x^{24} + 2x^{16} + 2x^{12} + 2x^8 + x^4 + 1 \\ = {} & (x^{48} + x^{40} + 2x^{36} + 2x^{32} + 2x^{28} + x^{24} + x^{20} + 2x^{16} + 2x^{12} + 2x^8 \\ & + 2x^4 + 2)^2 (x^{48} + 2x^{44} + 2x^{36} + x^{32} + 2x^{28} + x^{24} + x^{20} + x^{16} \\ & + 2x^{12} + 2x^4 + 2)^2. \end{aligned}$$

4.3. Composed addition

Let $G \subset \Gamma_q$ be a subgroup of the additive group of Γ_q, and select irreducibles f, $g \in M_G[q,x]$ of degrees m and n, respectively, and with roots α and β, respectively. Set $d = \gcd(m,n)$ and $h = \operatorname{lcm}(m,n)$, and suppose that for some $k \in \{1,2,\ldots,h-1\}$ and $i \in \{1,2,\ldots,d-1\}$ we have $(\alpha+\beta)^{q^k} = \alpha + \beta^{q^i}$. Note from Theorem 4.1 that k and $k-i$ are multiples of $\deg(\alpha - \alpha^{q^d})$ and $\deg(\beta - \beta^{q^d})$, respectively, and that the partial converse given in Theorem 4.2 can be modified by considering the factors of the affine q-polynomials $v_\gamma(x) = x^{q^k} - x - \gamma$ and $w_\gamma(x) = x^{q^i} - x^{q^k} - \gamma$, where $v_\gamma(x)$, $w_\gamma(x) \in \mathbb{F}_{q^d}[x]$ (see [4] for a discussion of q-polynomials). This adaptation results in the following theorem.

Theorem 4.9. *Let G be a subgroup of $(\Gamma_q,+)$ and let $d \in \mathbb{Z}^+$ and $\gamma \in \mathbb{F}_{q^d}$ be given. Select positive integers k and i where $i < d$. If $\alpha,\beta \in G$ satisfy $v_\gamma(x)$ and $w_\gamma(x)$, respectively, then the degrees of α and β over $\mathbb{F}_q$ divide pdk_1 and $pd(k-i)_1$, respectively, where $p = \operatorname{char}(\mathbb{F}_q)$ and k_1 and $(k-i)_1$ are defined as in Theorem* 4.2.

Example 4.10. We work over $\mathbb{F}_3$ in this example. Let $k=5$, $i=2$, $d=3$ and $\gamma=2$; thus $v_2(x) = x^{243} - x - 2$ and $w_2(x) = x^9 - x^{243} - 2$. Hence by Theorem 4.9, $\alpha,\beta \in \Gamma_3$ must have degrees dividing 45 and 9, respectively. We select a factor $f(x) = x^{15} + x^{13} + x^{12} + x^{11} + 2x^{10} + 2x^9 + 2x^7 + 2x^5 + 2x^4 + x^3 + x^2 + 2x + 1$ from v_2 and a factor $g(x) = x^9 + 2x^6 + 2x^4 + x^3 + 2x^2 + x + 2$ from w_2. We have

$$\begin{aligned} f * g &= x^{135} + x^{126} + x^{120} + x^{117} + x^{114} + 2x^{108} + 2x^{102} + 2x^{96} \\ &\quad + 2x^{93} + 2x^{90} + 2x^{87} + x^{84} + 2x^{81} + x^{72} + x^{66} + x^{60} + 2x^{57} \\ &\quad + x^{54} + 2x^{45} + x^{39} + x^{36} + 2x^{33} + x^{30} + 2x^{24} + x^{21} + 2x^{18} \\ &\quad + 2x^{15} + x^{12} + x^9 + x^6 + 2x^3 + 1 \\ &= (x^{45} + x^{42} + x^{40} + x^{39} + x^{38} + 2x^{36} + 2x^{34} + 2x^{32} + 2x^{31} \\ &\quad + 2x^{30} + 2x^{29} + x^{28} + 2x^{27} + x^{24} + x^{22} + x^{20} + 2x^{19} + x^{18} \\ &\quad + 2x^{15} + x^{13} + x^{12} + 2x^{11} + x^{10} + 2x^8 + x^7 + 2x^6 + 2x^5 \\ &\quad + x^4 + x^3 + x^2 + 2x + 1)^3. \end{aligned}$$

5. An open problem

For which prime powers q and positive integer pairs $m,n > 1$ does the following statement hold: For any $r \in \mathbb{Z}$, $1 \leqslant r \leqslant d$, there exist irreducibles $f,g \in M_G[q,x]$ of degrees m and n, respectively, such that the number of distinct irreducible factors in the factorization of $f \diamondsuit g$ is r? As we saw in Examples 4.8 and 4.10, it is possible for composed products of irreducibles of non-coprime degrees to have potentially far fewer than the maximum possible number of distinct factors.

Acknowledgements

The author gratefully acknowledges the advice and support of Joel Brawley and Shuhong Gao in the writing of this paper. He wishes to thank the anonymous referees as well for their helpful suggestions, with a special thanks to the referee who pointed out the relation of this work to the matter of determining the minimal polynomial of a product sequence. Maple as well as the number theory package pari were used in the computations.

References

[1] J.V. Brawley, L. Carlitz, Irreducibles and the composed product for polynomials over a finite field, Discrete Math. 65 (1987) 115–139.
[2] J.V. Brawley, S. Gao, D. Mills, Computing composed products of polynomials, Contem. Math. 225 (1999) 1–15.
[3] D.D. Brown, Iterated presentations and module polynomials over finite fields, Ph.D. Thesis, Clemson University, 1990.
[4] R. Göttfert, H. Niederreiter, On the minimal polynomial of the product of linear recurring sequences, Finite Fields Appl. 1 (1995) 204–218.
[5] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and Applications, vol. 20, Addison-Wesley, Reading, MA, 1983 (now distributed by Cambridge University Press).